



2876

PATENT  
Attorney Docket No.: 4284.0829

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
**RECEIVED**

In re Application of:

TAKAFUMI WATANABE

**MAY 25 2000**

**GROUP 2700**

Serial No.: 09/498,995

Group Art Unit: 2876

Filed: February 7, 2000

Examiner: Unknown

For: PORTABLE ELECTRONIC  
DEVICE AND A METHOD FOR  
ISSUING THE DEVICE

**CLAIM FOR PRIORITY**

Assistant Commissioner for Patents  
Washington, D.C. 20231

**RECEIVED**

**APR 14 2000**

Sir:

TECHNOLOGY CENTER 2800

Under the provisions of 35 U.S.C. § 119, Applicant hereby claims the benefit of the filing date of Japanese Application No. 11-029976, filed February 8, 1999, for the above-identified U.S. patent application.

In support of Applicant's claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Date:

4/12/00

By:

Richard V. Burgujian  
Registration No. 31,744

LAW OFFICES

FINNEGAN, HENDERSON,  
FARABOW, GARRETT,  
& DUNNER, L.L.P.  
1300 I STREET, N. W.  
WASHINGTON, D. C. 20005  
202-408-4000



日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

053  
30030  
RECEIVED

MAY 25 2000

GROUP 2700

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日

Date of Application:

1999年 2月 8日

出願番号

Application Number:

平成11年特許願第029976号

出願人

Applicant (s):

株式会社東芝

RECEIVED

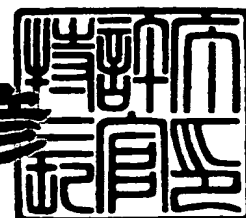
APR 11 2000

TECHNOLOGY CENTER 2800

2000年 1月21日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



出証番号 出証特2000-3000350

【書類名】 特許願

【整理番号】 A009807072

【提出日】 平成11年 2月 8日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 19/00

【発明の名称】 携帯可能電子装置

【請求項の数】 9

【発明者】

    【住所又は居所】 神奈川県川崎市幸区柳町 7 0 番地 株式会社東芝柳町工場内

    【氏名】 渡辺 隆文

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100084618

    【弁理士】

    【氏名又は名称】 村松 貞男

【選任した代理人】

    【識別番号】 100068814

    【弁理士】

    【氏名又は名称】 坪井 淳

【選任した代理人】

    【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書  
【発明の名称】 携帯可能電子装置  
【特許請求の範囲】

【請求項 1】 不揮発性メモリとセキュリティ機能を有する携帯可能電子装置において、

上記不揮発性メモリにセキュリティ機能を有効化するか否かを示すデータを記憶する記憶手段と、

外部から供給される電文のフォーマットがセキュリティ用のデータを含むフォーマットか否かを判断する第 1 の判断手段と、

上記記憶手段により上記不揮発性メモリにセキュリティ機能の有効化を示すデータが記憶されているか否かを判断する第 2 の判断手段と、

上記第 1 の判断手段により電文のフォーマットがセキュリティ用のデータを含まないフォーマットと判断し、上記第 2 の判断手段によりセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第 1 の実行手段と、

上記第 1 の判断手段により電文のフォーマットがセキュリティ用のデータを含むフォーマットと判断した際に、電文に基づいてセキュリティ機能による検証に成功したか否かを判断する第 3 の判断手段と、

この第 3 の判断手段によりセキュリティ機能による検証に成功したと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第 2 の実行手段と、

を具備したことを特徴とする携帯可能電子装置。

【請求項 2】 上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと書き込みおよび書き換える対象データとこの対象データの正当性を保証する補助データとからなり、上記セキュリティ機能は補助データの正当性の判断により行われることを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 3】 上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと暗号化されている書き込みおよび書き

換えの対象データとからなり、上記セキュリティ機能は暗号化されている対象データの復号化により行われることを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 4】 上記セキュリティ用のデータを含む電文のフォーマットが、書き込みおよび書き換えを示すコマンドと暗号化されている書き込みおよび書き換えの対象データとこの暗号化されている対象データの正当性を保証する補助データとからなり、上記セキュリティ機能は補助データの正当性の判断と、暗号化されている対象データの復号化により行われることを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 5】 上記不揮発性メモリに複数のアプリケーションが記憶され、上記セキュリティ機能はアプリケーション毎に独立して設定可能であることを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 6】 上記記憶手段に記憶されているセキュリティ機能を有効化するか否かを示すデータはセキュリティ機能を有効化する電文を受信した場合に有効化することを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 7】 上記不揮発性メモリに複数のアプリケーションファイルが記憶されており、各アプリケーションファイル毎に処理される電文フォーマットを指定する指定情報が設定されていることを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 8】 上記第 1 の判断手段にてセキュリティ用のデータを含むフォーマットと判断し、かつ、上記第 2 の判断手段にて上記記憶手段にセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、用不揮発性メモリに複数のアプリケーションが記憶され、上記セキュリティ機能許容フォーマットでない旨の応答ステータスを出力することを特徴とする請求項 1 に記載の携帯可能電子装置。

【請求項 9】 上記携帯可能電子装置は、IC モジュールにより構成されていることを特徴とする請求項 1 に記載の携帯可能電子装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ＩＣカード等の携帯可能電子装置に関する。

【０００２】

【従来の技術】

ＩＣカード等の携帯可能電子装置では、暗証番号の照合や送信データの暗号化などにて実現されるセキュリティ機能にて、内部メモリに格納されているデータを不正な第三者が読み出し・書き込み・書き換えが出来ないような管理を行っている。

【０００３】

ＩＣカードは、所有者の暗証番号や暗号鍵などのアプリケーション運用に必要なデータを書き込むことにより使用可能な状態となる。この書き込み行為は一般に発行と呼ばれる。この発行時には不特定多数のカードに大量のデータを書くこととなるが、書き込みのためにはＩＣカードで要求されているセキュリティ機能を満足する必要がある、データの暗号化など事前処理などを行うこととなるので非効率的である。

【０００４】

この結果、発行以前のカードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させることにより、それ以降のデータ書き込み・書き換えにはカードの要求するセキュリティ機能の実現ができるものが要望されている。

【０００５】

すなわち、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となるＩＣカードが要望されている。

【０００６】

【発明が解決しようとする課題】

この発明は、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となるものが要望されているもので、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計るこ

とが可能となる携帯可能電子装置を提供することを目的としている。

【0007】

【課題を解決するための手段】

この発明の携帯可能電子装置は、不揮発性メモリとセキュリティ機能を有するものにおいて、上記不揮発性メモリにセキュリティ機能を有効化するか否かを示すデータを記憶する記憶手段と、外部から供給される電文のフォーマットがセキュリティ用のデータを含むフォーマットか否かを判断する第1の判断手段と、上記記憶手段により上記不揮発性メモリにセキュリティ機能の有効化を示すデータが記憶されているか否かを判断する第2の判断手段と、上記第1の判断手段により電文のフォーマットがセキュリティ用のデータを含まないフォーマットと判断し、上記第2の判断手段によりセキュリティ機能の有効化を示すデータが記憶されていないと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第1の実行手段と、上記第1の判断手段により電文のフォーマットがセキュリティ用のデータを含むフォーマットと判断した際に、電文に基づいてセキュリティ機能による検証に成功したか否かを判断する第3の判断手段と、この第3の判断手段によりセキュリティ機能による検証に成功したと判断した際に、電文に基づいて不揮発性メモリに対する書き込みおよび書き換え処理を実行する第2の実行手段とからなる。

【0008】

【発明の実施の形態】

以下、この発明の実施形態について図面を参照して説明する。

【0009】

図1は、この発明のICカード（携帯可能電子装置）2を処理するICカード処理装置1の全体構成を示すブロック図である。

【0010】

このICカード処理装置1には、装置全体の制御を司る端末3が設けられている。この端末3には、ICカード2と端末3とを接続可能にし、ICカード2とデータのやり取りを行うカードリーダー/ライタ4、コマンドやその他のデータを入力するキーボード5、各種データを表示するCRTディスプレイ6、各種デー



タを印刷出力するプリンタ 7、各種データを記憶するフロッピーディスク装置 8 がそれぞれ接続されている。上記カードリーダー/ライタ 4 は、コネクタ等の接触式あるいはアンテナを用いる無線式により、IC カード 2 とデータのやり取りを行うようになっている。

【0 0 1 1】

図 2 は、IC カード 2 の機能を概略的に示すブロック図である。すなわち、IC カード 2 は、リーダー/ライタ部 1 1、暗証設定/暗証照合部 1 2、暗号化/復号化部 1 3 等の基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ 1 0 から構成されている。

【0 0 1 2】

上記リーダー/ライタ部 1 1 は、上記端末 3 からカードリーダー/ライタ 4 を介して供給されたコマンド、データ等に基づき後述するデータメモリ 1 5 あるいはプログラムメモリ 1 6 からデータを読取ったり、書込んだりするものである。

【0 0 1 3】

上記暗証設定/暗証照合部 1 2 は、暗証を設定したり暗証の照合を行うものである。

【0 0 1 4】

上記暗号化/復号化部 1 3 は、上記端末 3 へ供給するデータを暗号化したり、上記端末 3 から供給された暗号化データを復号化するものである。

【0 0 1 5】

スーパーバイザ 1 0 は、上記端末 3 からカードリーダー/ライタ 4 を介して供給された機能コードもしくはデータの付加された機能コードを解釈し、実行させるものである。

【0 0 1 6】

上記諸機能を発揮させるために IC カード 2 は、図 3 に示すように、全体を制御する制御素子 1 4 とデータメモリ 1 5 とプログラムメモリ 1 6 とコンタクト部 1 8 からなる物理構成となっている。

【0 0 1 7】

データメモリ 1 5 は、各種データの記憶に使用され E E P R O M (不揮発性メ

メモリ)で構成されている。プログラムメモリ16はマスクROMで構成されたものであり、制御プログラムがあらかじめ記憶されているものである。コンタクト部18は外部(カードリーダー/ライタ4)との接点となるものである。

#### 【0018】

上記制御素子14、データメモリ15、プログラムメモリ16は1チップ状のIC20として形成されており、このIC20に外部とのインターフェイス部としてのコンタクト部18が接続されて一体化(モジュール化)されたICモジュール21がプラスチックカードに埋め込まれることによりICカード2が形成されている。

#### 【0019】

図4は、上記データメモリ15の構成を示す図である。ICカード2の運用時におけるデータメモリ15のマッピング例である。

#### 【0020】

すなわち、データメモリ15は、システムエリア15a、DF(ディジネテッドファイル)、EF(エレメンタリーファイル)定義エリア15b、データエリア15cの3つの領域からなる。

#### 【0021】

システムエリア15aは、ICカード2が動作する上で必須な固定データおよび可変データの初期値から構成されている。システムエリア15aは、ICカード2を運用するためには必須の領域であり、初期化時にデータが書き込まれている。

#### 【0022】

DF、EF定義エリア15bは、DFの定義情報と、このDFの子供に対応する少なくとも1つのEF定義情報とが記録されるものである。図4の場合、DF1の定義情報に対して、EF1-1、EF1-2の2つのEFの定義情報が記録されている。この場合、DF1定義情報は、DF名”DF1”のDF定義情報である。EF1-1定義情報およびEF1-2定義情報は、それぞれEF識別子”EF1”および”EF2”のEF定義情報であり、双方ともにDF1の配下に存在するものとする。DF、EF定義エリア15bの未使用エリアは、新規に創成

されるDFおよびEFのための領域である。

【0023】

また、データエリア15cは、各EF定義情報で管理されるデータ本体が格納されている領域である。

【0024】

データエリア15cには、複数のアプリケーションが記憶され、各アプリケーションごとにDF定義情報が付与されていることにより、アプリケーション毎に独立してセキュリティ機能の有効、無効を設定可能である。

【0025】

図5を用いて上記DF定義情報の構成例を説明する。

【0026】

上記DF定義情報は、DF名21、DFサイズ情報22、セキュリティフォーマット情報23、セキュリティフラグ24により構成されている。

【0027】

DF名21はDF毎にユニークな情報であり、この情報により処理対象のDFの検索を行う。DFサイズ情報22は当該ファイルが使用可能なデータメモリ15の情報であり、当該DF配下にEFを創成した場合、その際に使用したサイズが当情報より減算される。セキュリティフォーマット情報23は当該DF配下における書き込みおよび書き換え系コマンドの実現されるべき電文フォーマット（後述する）の情報が設定されている。

【0028】

セキュリティフラグ24は当DF定義情報が有効化されている際に立つものであり、このフラグにより当DF定義情報が有効化されている場合に、当該DF配下における書き込みおよび書き換え系コマンドではセキュリティフォーマット情報23で指定される電文フォーマットは許可され、それ以外の電文フォーマットは拒絶されるものである。

【0029】

図6を用いて上記DF配下に構築されるEF定義情報の構成例を説明する。

【0030】

EF定義情報は、DF識別情報31、EF識別子32、アドレス情報33、EFサイズ情報34、EFフォーマット情報35により構成されている。

#### 【0031】

DF識別情報31は当該EFがどのDFの配下に存在するかを識別する情報である。EF識別子32は各EF毎にユニークな情報であり、この情報により処理対象のEFを検索する。アドレス情報33は当該EF制御情報で管理されるデータ格納領域の物理的アドレスを示す。EFサイズ情報34は当該EF制御情報で管理されるデータ格納領域のサイズ情報を示す。EFフォーマット情報35は当該EF制御情報が、例えば、ISO7816-4で規定されているレコード構造EFかあるいはトランスペアレント構造EFなのかの情報を与えるものである。

図7の(a)～(d)を用いて書き込みおよび書き換え系コマンドの実現されるべき電文フォーマットを説明する。

#### 【0032】

図7の(a)に示すフォーマット#1は、書き込みおよび書き換え系コマンドの基本的なフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と書き込みおよび書き換えの対象データとしてのデータ部とからなり、上記のセキュリティフラグ24が有効化されていない場合にのみ許容されるものである。

#### 【0033】

図7の(b)に示すフォーマット#2は、データの隠蔽性を実現するために暗号化データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と暗号化されている書き込みおよび書き換えの対象データとしての暗号化データ部とからなる。このフォーマットの場合、暗号化されている書き込みおよび書き換えの対象データの復号化によりセキュリティ機能の検証が行われる。

#### 【0034】

図7の(c)に示すフォーマット#3は、データの正当性を実現するために補助データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と書き込みおよび書き換えの対象データとしてのデ

ータ部と対象データの正当性を保証する補助データ部とからなる。このフォーマットの場合、補助データの正当性の判断によりセキュリティ機能の検証が行われる。

【 0 0 3 5 】

図 7 の ( d ) に示すフォーマット # 4 は、データの隠蔽性および完全性を実現するために暗号化データ部を有し、かつ、補助データ部を有するフォーマットであり、書き込みおよび書き換えを示すコマンドとしてのコマンドヘッダ部と暗号化されている書き込みおよび書き換えの対象データとしての暗号化データ部と暗号化されている対象データの正当性を保証する補助データ部とからなる。このフォーマットの場合、暗号化されている書き込みおよび書き換えの対象データの復号化と、補助データの正当性の判断とによりセキュリティ機能の検証が行われる。

【 0 0 3 6 】

上記フォーマット # 1 ~ # 3 は、上記セキュリティフォーマット情報 2 3 にて各 D F 毎に指定されるようになっている。

【 0 0 3 7 】

図 8 に上記セキュリティフラグ 2 4 を有効化するコマンドの電文フォーマットを示す。このコマンドは、コマンドヘッダ部のみにより構成されている。

【 0 0 3 8 】

当該コマンドが実行された直後より、D F 定義情報のセキュリティフラグ 2 4 が有効化されるようになっている。

【 0 0 3 9 】

次に、D F 定義情報のセキュリティフラグ 2 4 を有効化する処理を、図 9 に示すフローチャートを参照しつつ説明する。

【 0 0 4 0 】

すなわち、端末 3 からセキュリティフラグを有効化するコマンドの電文（図 8 参照）が、カードリーダー/ライタ 4 をコンタクト部 1 8 を介して I C カード 2 内の制御素子 1 4 に送信される。これにより、制御素子 1 4 は端末 3 から送信された電文を受信し（S T 1）、この受信した電文が、セキュリティフラグを有効化

するコマンドと判断した際に（ST2）、現在処理中（カレント状態）のDF定義情報内のセキュリティフラグ24を有効化する（ST3）。

【0041】

次に、書き込みおよび書き換え系コマンドによる処理を、図10に示すフローチャートを参照しつつ説明する。

【0042】

すなわち、端末3から書き換えおよび書き込み系コマンドの電文（図7の（a）～（d）参照）が、カードリーダーライタ4をコンタクト部35を介してICカード2内の制御素子14に送信される。これにより、制御素子14は端末3から送信された電文を受信し（ST11）、この受信した電文フォーマット内容进行判断する（ST12）。これにより、制御素子14は、図7の（a）に示すフォーマット#1と判断した際に、現在処理中（カレント状態）のDF定義情報内のセキュリティフラグ24を有効化済みか否かを判断する（ST13）。この判断により、セキュリティフラグ24を有効化済みでないと判断された際に、制御素子14は、コマンドヘッダ部により指定されている書き換えおよび書き込み処理を実行する（ST14）。

【0043】

これにより、発行以前のICカード2において、要求されているセキュリティ機能を実現せずに、データの書き換えおよび書き込みが行うことができ、発行時の効率化を計ることが可能となる。

【0044】

また、上記ステップ13によりセキュリティフラグ24を有効化済みと判断された際に、制御素子14は、「許容フォーマットでない」の応答ステータスを端末3へ送信する（ST15）。これにより、フォーマット#1は、当該DF制御情報のセキュリティフラグ24が有効化されている場合に拒絶される。

【0045】

また、上記ステップ12により電文がフォーマット#1と判断しなかった際に、制御素子14は、現在処理中（カレント状態）のDF定義情報内のセキュリティフォーマット情報23に基づいて指定される処理を、受信した電文を用いて実

施する (ST16)。

【0046】

この処理により、制御素子14は、セキュリティ機能による検証に成功したか否かを判断する (ST17)。この判断の結果、セキュリティ機能による検証に成功した際、制御素子14は、コマンドヘッダ部により指定されている書き換えおよび書込み処理を実行する (ST14)。

【0047】

これにより、ICカード2の発行後のデータ書き込み・書き換えに対して、カードの要求するセキュリティ機能を実現できる。

【0048】

また、上記ステップ17によりセキュリティ機能による検証に成功しなかった際に、制御素子14は、「受信した電文の正当性の検証に失敗」の応答ステータスを端末3へ送信する (ST18)。

【0049】

上記したように、発行以前のICカードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させることにより、それ以降のデータ書き込み・書き換えにはICカードの要求するセキュリティ機能の実現が必須となる。すなわち、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる。

【0050】

【発明の効果】

以上詳述したように、この発明によれば、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる携帯可能電子装置を提供できる。

【図面の簡単な説明】

【図1】

この発明のICカード処理装置の全体構成を示すブロック図。

【図2】

ICカードの機能を概略的に示すブロック図。

【図 3】

ICカードの構成を概略的に示すブロック図。

【図 4】

データメモリの構成を示す図。

【図 5】

DF 定義情報の構成例を示す図。

【図 6】

EF 定義情報の構成例を示す図。

【図 7】

書き込みおよび書き換え系コマンドの実現されるべき電文フォーマットを示す図。

【図 8】

セキュリティフラグを有効化するコマンドの電文フォーマットを示す図。

【図 9】

DF 定義情報のセキュリティフラグを有効化する処理を説明するためのフローチャート。

【図 1 0】

書き込みおよび書き換え系コマンドによる処理を説明するためのフローチャート。

【符号の説明】

1 … ICカード処理装置

2 … ICカード（携帯可能電子装置）

3 … 端末

4 … カードリーダー／ライター

1 1 … リーダー／ライター

1 4 … 制御素子

1 5 … データメモリ

1 5 a … システムエリア

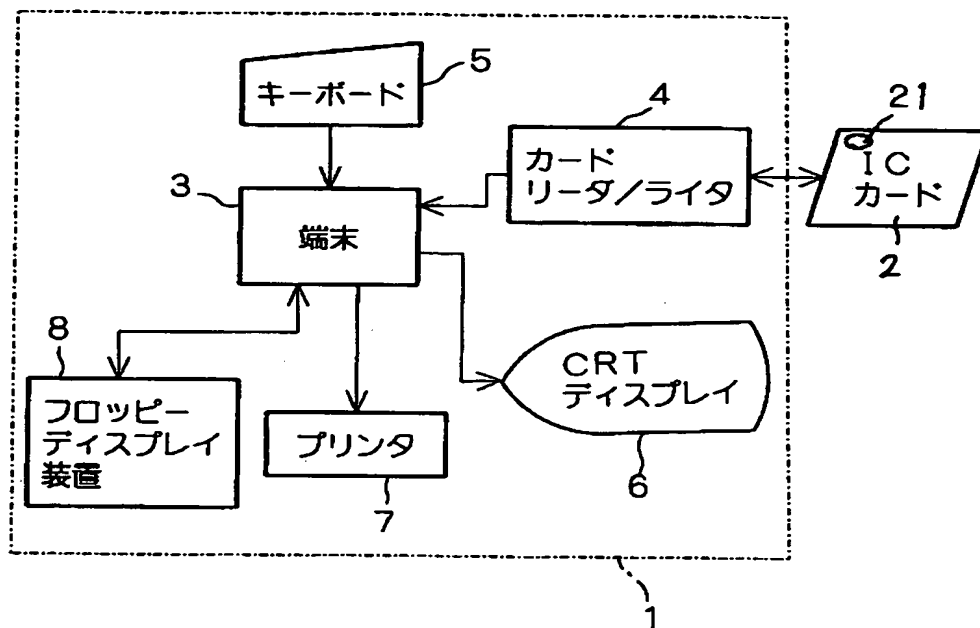


15b...DF、EF定義エリア

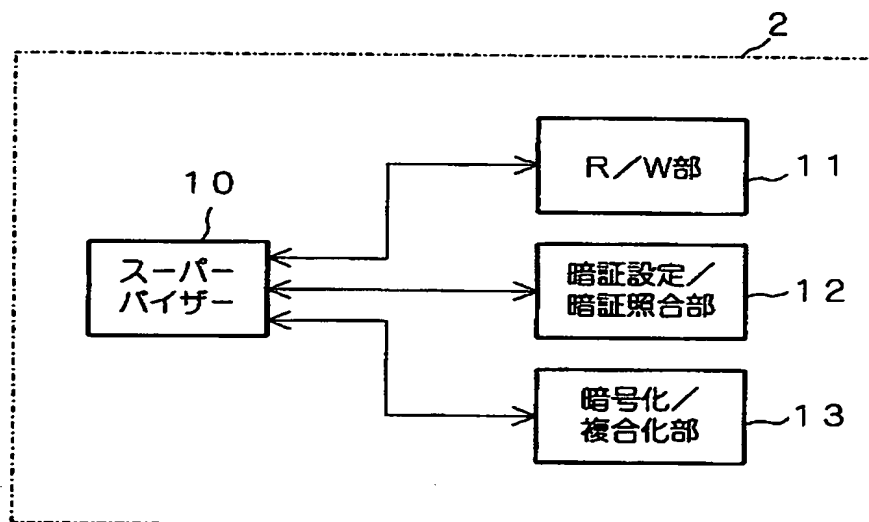
15c...データエリア

【書類名】 図面

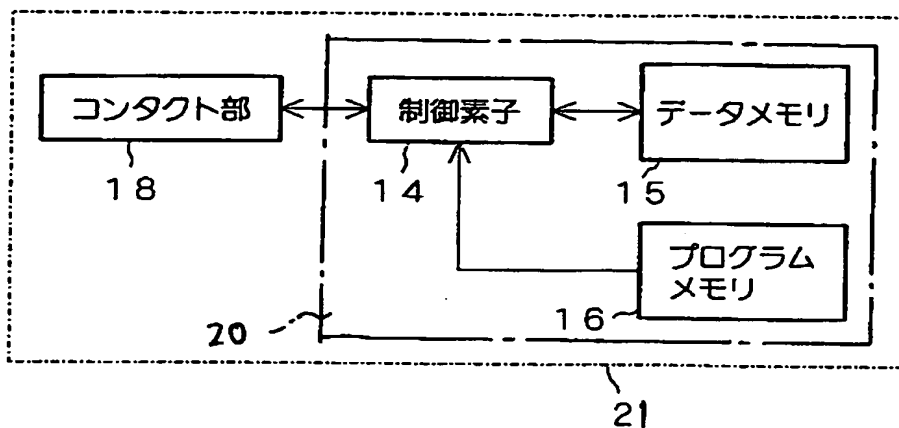
【図 1】



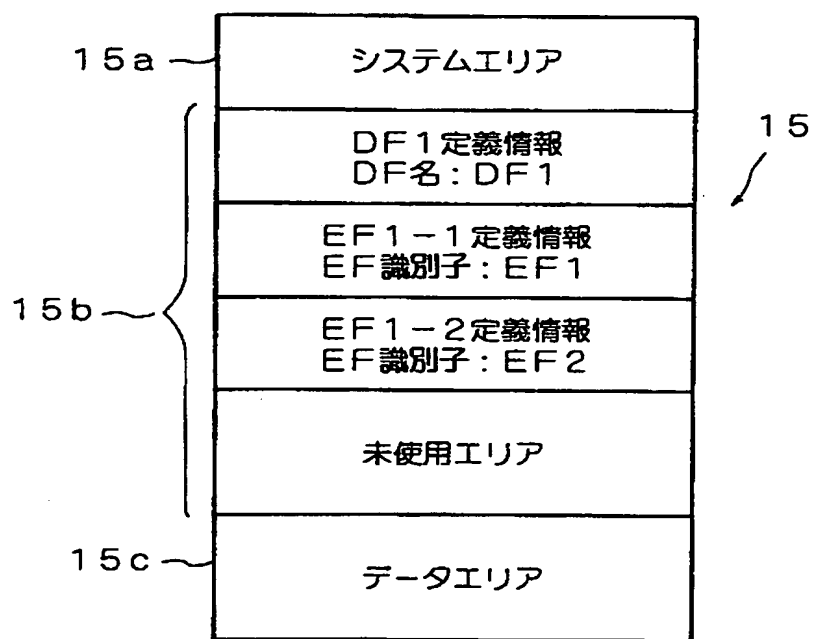
【図 2】



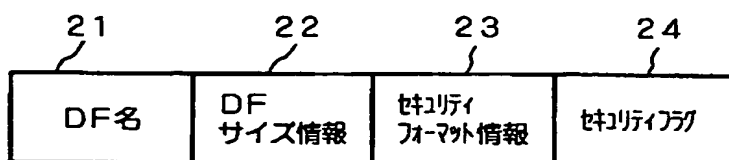
【図 3】



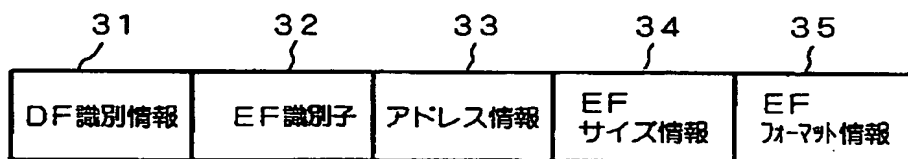
【図 4】



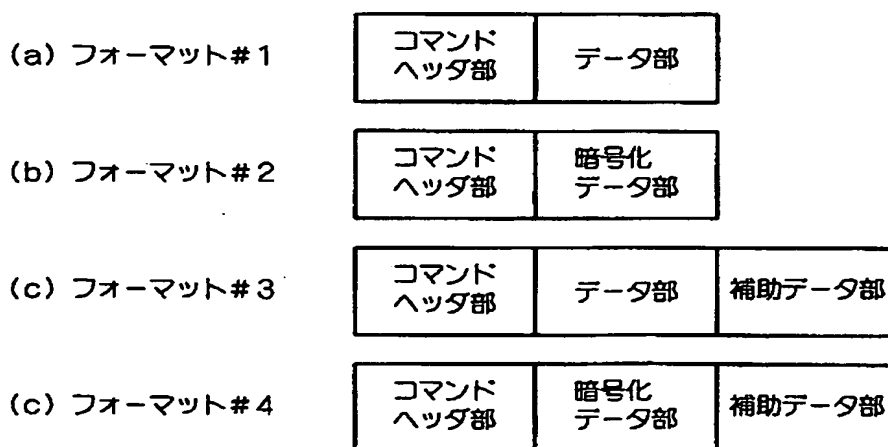
【図 5】



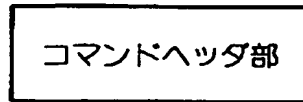
【図 6】



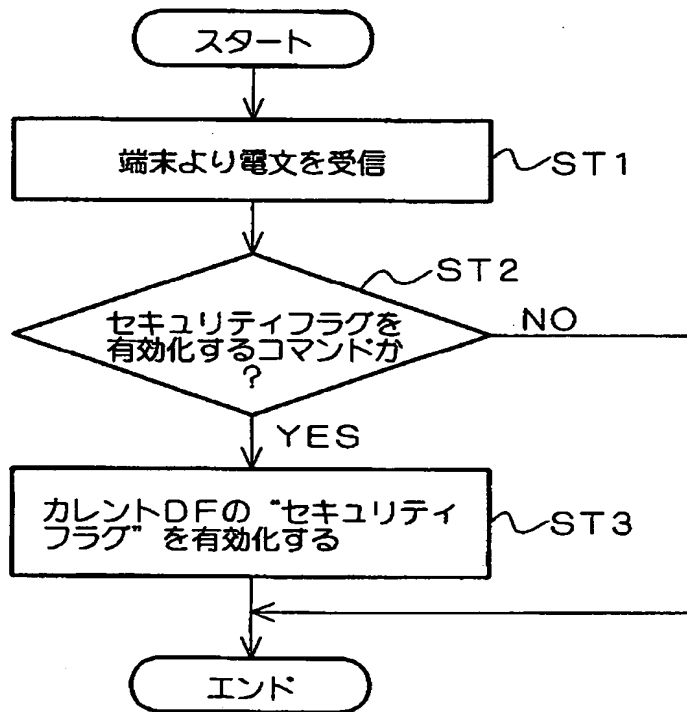
【図 7】



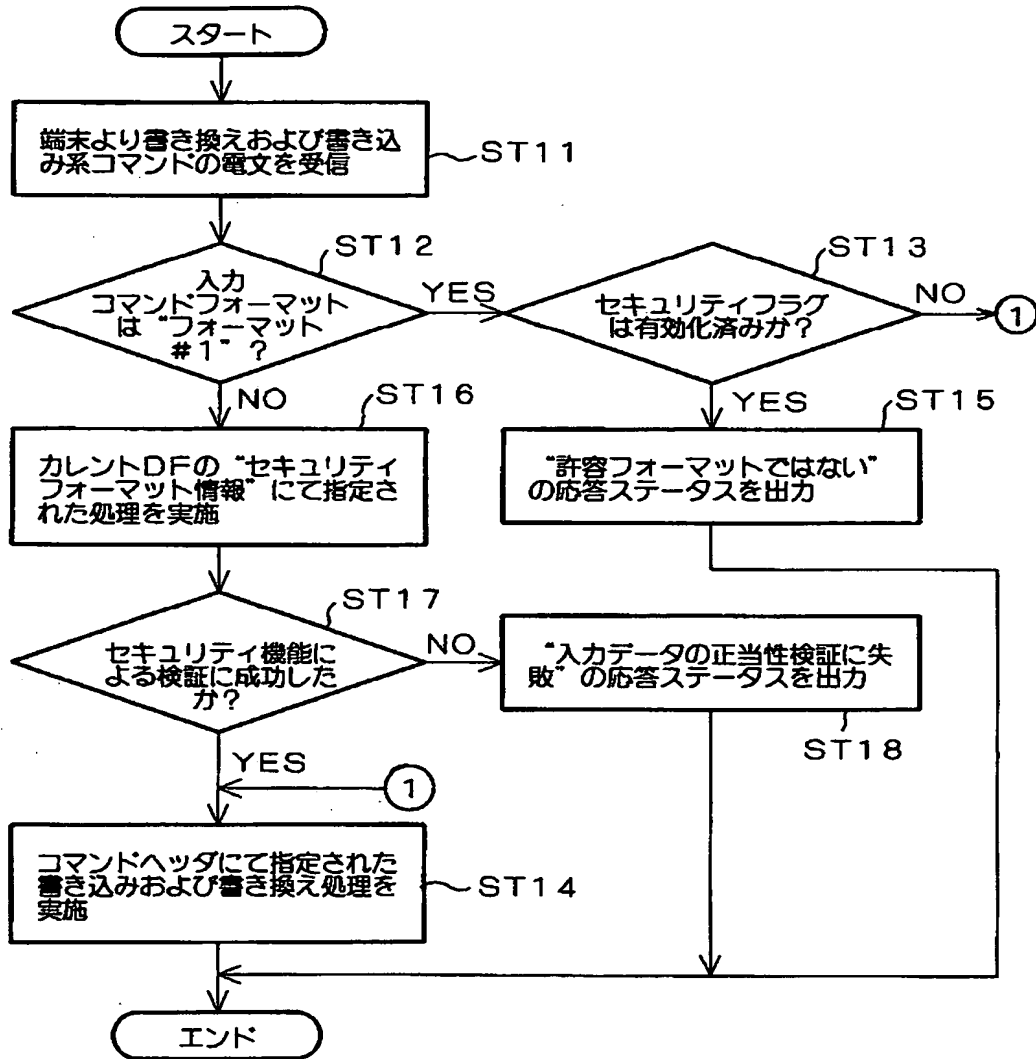
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 この発明は、アプリケーション運用時には高セキュリティを実現でき、かつ、発行時の効率化を計ることが可能となる。

【解決手段】 この発明は、発行以前の IC カードでは要求されているセキュリティ機能を実現せずともデータの書き込みが行うことができ、すべてのデータが書き込まれた後にセキュリティ機能を有効化させるようにしたものである。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝